CLAIMS

We claim:

1. A method for improving the operation of equipment used to protect a web server against attack, comprising the acts of:

reading a source address of a message received during an attack;

checking a database of privileged source addresses; and

instructing protective equipment for a web server to pass the received message to the web server when the source address of the received message matches an address contained in the database of privileged source addresses.

2. The method of claim 1, wherein the database of privileged source addresses includes a source address of a customer known to the web server.

3. The method of claim 1, wherein the database of privileged source addresses includes a source address of a user known to the web server.

4. A method for improving the operation of equipment used to protect a web server against attack by a vandal, comprising the acts of:

reading a source address of a message received during an attack;

checking a database of privileged source addresses for appearance of the source address of the received message;

when the source address of the received message appears in the database of privileged source addresses, instructing protective equipment to pass the received message to a web server;

when the source address of the received message does not appear in the database of privileged source addresses, checking a database of blocked source addresses for appearance of the source address of the received message; and

when the source address of the received message does not appear in the database of blocked source addresses, adding the source address of the received message to the database of blocked source addresses and instructing the protective equipment to block the received message and to block subsequent messages that bear the source address of the received message.

5. Protective equipment for guarding a web server against attack, comprising:

an address decoder for reading a source address of a message received during an attack;

a database of privileged source addresses; and

logic for instructing protective equipment for a web server to pass the message received during the attack to the web server when the source address of the message received during the attack matches a privileged source address contained in the database of privileged source addresses.

6. The intrusion detection security system of claim 5, wherein the database of privileged source addresses includes a source address of a customer known to access the web server.

7. The intrusion detection security system of claim 5, wherein the database of privileged source addresses includes a source address of a known users of the web server.

8. Protective equipment for guarding a web server against attack, comprising:

an address decoder for reading a source address of a message received during an attack;

a database of privileged source addresses;

a database of blocked source addresses; and

logic for checking the database of privileged source addresses and the database of blocked source addresses for appearance of the source address of the message received during the attack and, responsive to the appearance, instructing protective equipment to block incoming messages that bear the source address of the message received during the attack.

9. Protective equipment for guarding a web server against attack, comprising:

an address decoder for reading a source address of a message received during an attack;

a database of privileged source addresses;

a database of blocked source addresses; and

logic for:

checking the database of privileged source addresses for appearance of the source address of the received message;

when the source address of the received message appears in the database of privileged source addresses, instructing protective equipment to pass the received message to a web server;

when the source address of the received message does not appear in the database of privileged source addresses, checking the database of blocked source addresses for

appearance of the source address of the received message; and

When the source address of the received message does not appear in the database of blocked source addresses, adding the source address of the received message to the database of blocked source addresses and instructing the protective equipment to block the received message and to block subsequent messages that bear the source address of the received message.